UNITED STATES DISTRICT COURT

for the

Eastern District of California

United States of America
v.

SEAN THOMAS DELAPP

Defendant(s)

Case No. 2:23-mj-0126 CKD

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of August 24, 2023 in the county of Solano in the Eastern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 111(b)(1)	Assault on Federal Officer with a Deadly Weapon

This criminal complaint is based on these facts:

See Affidavit of FBI Special Agent Jose Gonzalez, attached hereto and incorporated by reference.

☒ Continued on the attached sheet.

/s/

Complainant's signature

Jose Gonzalez, FBI Special Agent

Printed name and title

Sworn to me and signed via telephone.

Date: September 5, 2023 at 11:54 am

Carolyn K. Delaney

Judge's signature

City and state: Sacramento, CA

Carolyn K. Delaney, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT, ARREST WARRANT, AND SEARCH WARRANTS

I, Jose Gonzalez, being duly sworn, depose and state:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the following person, residence, and vehicle:

I. PURPOSE

Attachment	Target	Process Sought
A-1	SEAN THOMAS DELAPP	Complaint, Arrest Warrant, & Search Warrant
A-2	532 Wallace Avenue, Vallejo, California	Search Warrant
A-3	A 2013 Mercedes Benz bearing California license plate 8FFS939	Search Warrant

2. This person and property are further described in Attachments A-1 through A-3. The applications seek to search them for the things described in Attachment B-1 through B-3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 111(b) – assault on a federal officer with a deadly weapon, and 18 U.S.C. § 922(g)(1) – felon in possession of firearms or ammunition have been committed by DELAPP. Collectively the violations described above will be referred to as the "TARGET OFFENSES." This affidavit also supports my application for a complaint and an arrest warrant of DELAPP for Assault on Federal Officer with a Deadly Weapon, in violation of 18 U.S.C. § 111(b)

II. AFFIANT'S BACKGROUND

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since June 2021. I graduated from the FBI Academy in Quantico, Virginia in October 2021. During the Basic Field Training course, I learned the necessary skills, tactics, and techniques needed to perform my investigative duties as an FBI Special Agent. I also learned how to conduct investigations of criminal activity, execute search and arrest warrants and seize evidence of violations of United States law.

4. I am currently assigned to the FBI' Sacramento Field Office, Fairfield Resident Agency,

where I have worked on and participated in a variety of cases; to include white collar crimes, bank robberies, child sexual exploration, illegal firearm and drug trafficking, threatening communications, identity theft, and hoaxes designed to elicit a law enforcement response. I have received training and I have gained experience in interviewing and interrogation techniques, arrest procedure, physical surveillance, search warrant applications, the execution of search and seizures, computer evidence seizure and processing, social media analysis and various other criminal laws and procedures. I have testified in federal grand juries and executed search and arrest warrants.

5. As a result of my training and experience with the FBI and conversations I have had with other law enforcement officers, I am familiar with the federal laws pertaining to firearms. I know it is unlawful under Title 18 of the United States Code for a previously convicted felon to possess a firearm or ammunition. As a result of my training and experience with the FBI and conversations I have had with other law enforcement officers, I know a firearm is a deadly or dangerous weapon if it is used in a way that is capable of causing death or serious bodily injury.

6. I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am an officer of the United States empowered by law to conduct criminal investigations and make arrests for offenses enumerated in 18 U.S.C. § 2516.

7. Because this affidavit is submitted for the limited purpose of establishing probable cause for the requested arrest warrant, I have not included each and every fact known to me about this case. Rather, I have set forth only the facts that I believe are necessary to support probable cause.

8. This affidavit is based upon my own personal knowledge but also the knowledge of other law enforcement officers involved in this investigation. Where I describe statements made by other people (including other special agents and law enforcement officers), the statements are described in sum, substance, and relevant part. Similarly, where I describe information contained in reports and other documents or records in this affidavit, this information is also described in sum, substance, and relevant part.

III. STATEMENT OF PROBABLE CAUSE

9. Victim 1 and Victim 2 are both Special Agents with the FBI and are assigned to the FBI's San Francisco Field Office.

10. On August 24, 2023, Victim 1 and Victim 2 were scheduled to meet N.K. regarding a case where a gun was found in N.K.'s car in 2019. N.K. was supposed to meet Victim 1 and Victim 2 at a Starbucks in Vallejo, California. N.K. did not show up to the scheduled meeting, so Victim 1 and Victim 2 drove to N.K.'s residence at an address on Humboldt Street, in Vallejo, California.

11. Victim 1 knocked on the door of the residence and T.D. opened the door. Victim 1 and Victim 2 identified themselves as FBI Agents and both showed their FBI credentials to T.D. T.D. stated that he was N.K.'s father. When Victim 1 was speaking with T.D., he received a phone call from N.K. T.D. told Victim 1 that N.K. did not want to talk to Victim 1 or Victim 2, and N.K. wanted them to leave. Victim 1 and Victim 2 went back to their FBI vehicle, which was parked on the residence side of the street approximately two houses down from the residence.

12. At approximately, 9:50 A.M., a white adult male, later identified as SEAN THOMAS DELAPP, driving a black Mercedes-Benz, drove slowly past the Victims' vehicle northbound on Humboldt Street. The plate of the Mercedes-Benz was partially identified as 8FFS. The Mercedes-Benz drove outside of the Victims' view near the residence on Humboldt Street. The Mercedes-Benz, driven by DELAPP, was later identified as a black 2013 Mercedes-Benz sedan bearing California license plate 8FFS939.

13. A few minutes later, Victim 1 and Victim 2 were sitting in their vehicle when the Mercedes-Benz came up from behind them and parked in front of other parked cars that were in front of their vehicle. DELAPP walked up to the passenger side of the Victims' vehicle and knocked on the passenger front window. Victim 1 lowered the window down and DELAPP leaned into the Victims' vehicle and asked Victim 1, "what do you want?" Victim 1 said that she had some questions for N.K. DELAPP asked Victim 1 if she was [Victim 1's first name]. Victim 1 answered yes. DELAPP said N.K. was not answering any questions. DELAPP identified himself as N.K.'s brother.

14. Victim 1 and Victim 2 told DELAPP to back up as they got out of their vehicle. DELAPP asked Victim 1 and Victim 2 who they were, and they stated they were with the FBI. DELAPP asked to see identification. As Victim 1 and Victim 2 were pulling out their credentials, DELAPP pulled out his cell phone and appeared to record a video of Victim 1 and Victim 2. As Victim 1 and Victim 2 got back into their vehicle, DELAPP walked behind the vehicle, took a video of the

license plate, and then walked over to the driver side, still with his phone out, appearing to be recording. DELAPP stated his uncle was the "top cop in California" and DELAPP was going to find Victim 1 and Victim 2 and figure out who they were.

15. Victim 1 and Victim 2 were able to drive away. DELAPP ran back to his car and began to follow them in the Mercedes-Benz. Victim 1 noticed the Mercedes-Benz following them from Tennessee Street onto I-80 eastbound. Victim 1 called 911 to request assistance. Victim 1 and Victim 2 notified Vallejo Police dispatch they were FBI Agents, gave a description of DELAPP and the Mercedes-Benz, and reported that the Mercedes-Benz was still following them. The Mercedes-Benz sped up and got behind the Victims' vehicle and they were able to confirm that it was DELAPP.

16. Victim 1 took State Route 37 westbound from I-80 eastbound, and DELAPP continued to follow. While on the highway, DELAPP swerved through traffic, attempting to come up along the driver and passenger side of the Victims' vehicle. In an attempt to evade DELAPP, the Victims took the SR-37 exit last minute but DELAPP cut through the lanes to stay behind the Victims' vehicle. Vallejo Police dispatch transferred the call to California Highway Patrol dispatch and, as DELAPP attempted to get close to the passenger side of the Victims' vehicle, the Victims were able to provide a full license plate of the Mercedes-Benz.

17. Vehicle traffic was stop-and-go as they approached the Mare Island over-crossing. When the two westbound lanes of SR-37 merged to one large westbound lane, DELAPP drove alongside the left side of the Victims' vehicle into the center divider. DELAPP had the right-side front window down in his vehicle and yelled something at Victim 1, which Victim 1 could not hear. DELAPP dropped back into Victim 1's blind spot and then accelerated along the left side of the Victims' vehicle again. As DELAPP pulled alongside the Victims' vehicle again, the Victims saw DELAPP had his right arm extended across the passenger seat with a black[1] handgun pointed at the Victims through the Mercedes-Benz's passenger window. DELAPP made a recoil gesture with the handgun and was shouting. The Victims could not hear DELAPP. The Victims were on the phone with the California

[1] On August 31, 2023, I spoke with Victim 1, who said she was not entirely sure about the color the handgun. She mentioned she had a hard time seeing the color through the tinted windows and said it may have been brown.

Highway Patrol when DELAPP pointed the handgun at them.

18. DELAPP then passed the Victims' vehicle and drove to the left shoulder of westbound SR-37 and fled the scene. The Victims described DELAPP as a white male, approximately 5'10", upper 30s, long gray hair pulled back in a low ponytail. DELAPP wore a green Oakland A's hat, dark Oakley sunglasses, a short grey sleeve shirt, shorts, and tennis shoes. DELAPP had tattoos down both of his arms. The Victims were later provided social media photos of DELAPP at the Fairfield Resident Agency and were able to positively identify the individual DELAPP.

19. I have reviewed DELAPP's criminal history, which includes a felony conviction for evading a peace officer in 2006, in violation of California Vehicle Code, Section 2800.2. As a previously convicted felon, DELAPP is prohibited from possessing firearms or ammunition.

20. On August 31, 2023, a series of open-source checks were conducted on DELAPP. An open-source record associated 707-319-1051 to DELAPP as of May 2023, with the address 532 Wallace Ave, Vallejo, CA 94590. A second open-source record associated 707-319-1051 to DELAPP as of April 4, 2023 with the address 532 Wallace Ave, Vallejo, CA 94590. A third record, from December 2016, associated 707-319-1051 to DELAPP. Additionally, an FBI Task Force Officer who played on the same recreational baseball team with DELAPP from approximately 2016 to 2021 reported that DELAPP provided this phone number to the manager of the baseball team.

21. One open-source records check associated 707-319-1051 to S.D. The open-source record lists S. D. as the "Most Current Information." The same open-source record also listed historical information for 707-319-1051 under which DELAPP is listed. Additionally, the record from 2016 lists a different telephone number for S.D. Open-source records checks revealed that S.D. is approximately 30 years older than DELAPP, shares his last name, and lives in the same residence, suggesting she may be his mother. Additionally, the Mercedes that DELAPP was driving on August 24, 2023 is also registered to S.D. Surveillance officers observed the Mercedes at the 532 Wallace Ave. residence on August 24, 2023, around 3 P.M. (after the assault), as well as on and multiple days thereafter. Based on my training and experience, individuals sometimes have their cell phones subscribed in family member's names or under a family plan.

22. On September 1, 2023, two phone calls were placed to 707-319-1051. The first call went

straight to a voicemail box. The automated voicemail message did not identify the owner of the number. The second call rang once and then went to the voicemail box.

23. On September 1, 2023, this Court authorized a warrant to obtain location information for this cellular phone. I started receiving data from the carrier on September 2, 2023. This data shows that this cellular phone has been located in the vicinity of the 532 Wallace Avenue address the majority of the time, consistent with DELAPP residing at this address. On September 2, 2023, the cellular phone location data showed the cellular phone in Fairfield, California near the same time the Mercedes hit on a license plate reader in Fairfield. On the same day, the cellular phone location data showed the cellular phone in Vallejo, California near the same time the Mercedes hit on a license plate reader in Vallejo, California.

24. The returns from the location search warrant for this phone number also confirmed the listed subscriber as S.D. at the address 532 Wallace Ave. However, analysis of the data, coupled with additional investigation (e.g., this phone number is registered to DELAPP on CashApp and Paypal), identified the probable user of the cellular phone as DELAPP. The analysis also identified S.D. (DELAPP's likely mother), from a telephone number ending in 1632, as a top caller for 707-319-1051.

IV. TRAINING AND EXPERIENCE REGARDING ILLEGAL FIREARMS ACTIVITY

25. I know from my training, experience, and discussions with other experience law enforcement officials that those who illegally possess, manufacture, and/or traffic in firearms frequently possess the following evidence of their unlawful activity on their electronic devices:

a) Information concerning where and from whom the person purchased firearms or firearm parts;

b) Information concerning where and to whom firearms or parts were sold or transferred;

c) Correspondence to and/or from actual or prospective sources or buyers;

d) Records and/or documents of mailings, shipping or delivery, whether by the United States Postal Service or other private delivery services;

e) Information concerning methods used to advertise the availability of their firearms or firearm parts for purchase;

f) Photos of their firearms or firearm parts;

g) Written, recorded oral, or digital communications with associates involved in the purchase/sale of firearms or firearm parts; and

h) Written statements showing profits made from the sale of firearms or firearm parts.

26. I know that those who illegally possess firearms often use cellular telephones to communicate with one another, either by voice or text message. The information stored in a mobile telephone used by illegal firearm possessors, traffickers, and/or manufacturers is evidence of the associations of the illegal firearm possessor, trafficker, and/or manufacturer, some of which are related to illegal possession and transfer. Cellular telephones also contain in their memory text messages sent, received, and drafted by the mobile telephone user. The text message history of a cellular telephone can contain evidence of illegal firearm possession, trafficking and/or manufacturing because it shows the communications or planned communications of a firearm possessor, trafficker, and/or manufacturer and the telephone numbers of those with whom the illegal firearm possessor, trafficker, and/or manufacturer communicated or intended to communicate.

27. Illegal firearms possessors, traffickers, and/or manufacturers sometimes leave voice messages for each other, and this is evidence both of their mutual association and possibly their joint criminal activity. Cellular telephones can also contain other user-entered data files such as "to-do" lists, which can provide evidence of crime when used by an illegal firearm possessor, traffickers and/or manufacturers. Cellular telephones can also contain photographic data files, which can be evidence of criminal activity when the user was an illegal firearm possessor, trafficker and/or manufacturer who took pictures of evidence of crime. Cellular telephone companies also store the data described in this paragraph on their own servers and associate the data with particular users' mobile telephones.

28. Based on my training and experience, I know that people who possess firearms often maintain photographs or videos of their firearms and ammunition on their cellular telephones, including photographs or videos of the possessor holding or firing the firearm.

29. I know that convicted felons are unable to possess a firearm and therefore these individuals tend to maintain a continual chain of communication with lookouts and co-conspirators to obtain firearms by illegal means or criminal activity. I also know that these communications are

primarily conducted by cellular telephones. I know that people who negotiate the sale of firearms will often use cell phones to contact co-conspirators to obtain additional quantities of firearms and/or narcotics. I also know that photos of firearms and currency are often stored on such devices. Cellular phones can also supply historical information about the dates, times, duration, number, destination, and location of telephone calls, messages, photographs, video, audio, and other information processed or stored by the cellular telephone.

30. It has been my experience that people engaged in criminal activities utilize cellular telephones to maintain contact, either by telephone calls and/or text messaging, with close associates and people they trust, to include associates in the criminal activities, and that they carry these cellular telephones with them during the course of their criminal activities. Moreover, it has been my experience that people engaged in such criminal activities utilize these cellular telephones to take photographs and videos of themselves, their criminal associates, and other items related to their criminal activities, in some cases from the proceeds from their criminal activities. Relating to the ever-evolving level of cellular telephone technology, particularly increased storage capacity, through my training and experience, I know that cellular telephones can regularly store contacts, call logs, text messages, multimedia files, voicemail messages, and location/GPS data months and in some cases years from the date of the phone's activation.

31. Those who illegally possess firearms often, intentionally or unintentionally, retain paperwork and evidence indicating the source of that firearm whether it be by purchase, theft, or other means.

V. TECHNICAL TERMS

32. Based on my training and experience, I use the following technical terms to convey the following meanings:

a) Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number,

date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b) b) Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c) c) Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d) d) GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such

navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e) PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f) IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term-IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.

g) Internet: The Internet is a global network of computers and other electronic devices that

communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h) Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

VI. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

33. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

34. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

35. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of

the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contains information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example,

information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

36. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

37. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

38. Because several people share the PREMISES as a residence, it is possible that the

PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. The warrant applied for would permit the seizure and review of DELAPP's phone (assigned number 707-319-1051), as well as any devices in or on DELAPP's room, vehicle, and person.

VII. CONCLUSION

39. Based on the foregoing information, I request that a criminal complaint and arrest warrant be issued for DELAPP, charging him with assault on a federal officer with a deadly weapon, in violation of 18 U.S.C. § 111(b). I also request that this Court issue the search warrants for the person and property identified in Attachments A-1 through A-3 for items identified in Attachment B.

VIII. REQUEST TO SEAL

40. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

41. I request that the Court order this affidavit and associated applications and warrants to be kept under seal until further order of the Court. This scope of this investigation is not yet known to its targets. Disclosure of its contents of this affidavit would seriously impede the investigation, by disclosing details of the government's investigation and evidence gathered in connection therewith or providing the subject(s) with an opportunity to destroy evidence, tamper with witnesses, or flee. Accordingly, I request that the Court issue an order sealing the Complaint, arrest warrant, and affidavit until further order of this Court.

//

42. I swear, under the penalty of perjury, that the foregoing statements are true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,

/s/
JOSE GONZALEZ
Special Agent
FBI

Subscribed and sworn to me via telephone on: September 5, 2023

The Honorable Carolyn K. Delaney
UNITED STATES MAGISTRATE JUDGE

/s/ Adrian T. Kinsella
Approved as to form by AUSA ADRIAN T. KINSELLA

United States v. Sean Thomas Delapp
Penalties for Criminal Complaint

COUNT 1:

VIOLATION:	18 U.S.C. § 111(a) and (b) – Assault on a Federal Officer
PENALTIES:	A maximum of up to 20 years in prison; or A fine of up to $250,000; or both a fine and imprisonment Supervised release of up to 3 years
SPECIAL ASSESSMENT:	$100 (mandatory on each count)